

REMARKS

Applicant has carefully reviewed the Office Action mailed August 2, 2007 and offers the following remarks.

Claims 1, 3, 5, 6, 9-11, 17, 20, and 24-31 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent Application Publication No. 2002/0034301 A1 to Andersson (hereinafter "Andersson") in view of U.S. Patent No. 6,529,992 B1 to Thomas et al. (hereinafter "Thomas"). Applicant respectfully traverses.

To establish *prima facie* obviousness, the Patent Office must show that, in combination, the cited references teach each and every element of the claimed invention as recited in the claims. If the Patent Office cannot establish obviousness, the claims are allowable.

Before addressing the rejections, Applicant provides a brief overview of a portable device as recited in the claims. The portable device is configured to interact with any number of host computing devices. In operation, the portable device will initially appear to a host computing device as a known device type, such as a storage device. The host computing device will be configured to interact with the portable device as the storage device. Upon such interaction, the host computing device will access indicia sufficient to identify the portable device as a second device type, such as a cryptographic service provider, and instruct the host computing device to configure itself to interact with the portable device as the cryptographic service provider. In one embodiment, portable devices equipped with processing capabilities may operate to provide processing for the services provided by the cryptographic service provider on the portable device. In particular, the portable device may include a processing unit associated with the memory of the portable device that is used to provide the cryptography services to the host computing device, such that the portable device operates as a hardware-based cryptographic service provider.

Claim 1 recites a portable device for engaging a host computing device comprising:
a body;

a memory within the body containing:

initial identification indicia to initially identify the portable device to the host computing device as a storage device, which is known to the host computing device;

configuration indicia to subsequently identify the portable device to the host computing device as a cryptographic service provider and provide configuration

instructions to allow the host computing device to effectively interact with the portable device as the cryptographic service provider;

service indicia providing instructions to provide a service corresponding to the cryptographic service provider; and

an interface associated with the memory and adapted to facilitate interaction with the host computing device; and

a processing unit associated with the memory, wherein the service indicia includes instructions for the processing unit to provide the service corresponding to the cryptographic service provider to the host computing device.

Thus, as recited, such a single portable device can operate as both a known storage device and as a cryptographic service provider. In claim 1 (and in dependent method claim 29)¹, the portable device also includes a processing unit of the portable device, which is used to provide the cryptography service to the host computing device. As such, the portable device is initially identified as a known storage device to the host, and then runs configuration software from the portable device on the host device in order that the portable device can serve as a cryptographic service provider. In this way, the portable device is a true two-in-one device that performs both as a storage device and a cryptographic service provider.

Neither Andersson nor Thomas teaches or suggests such a two-in-one portable device that operates both as a storage device and as a cryptographic service provider. In addition, neither Andersson nor Thomas teaches or suggests where the portable device includes a processing unit associated with said memory, wherein the service indicia includes instructions for said processing unit to provide the service corresponding to the cryptographic service provider for the host computing device, as recited in claim 1. That is, neither Andersson nor Thomas teaches or suggests a portable device that operates as a hardware-based cryptographic service provider. Therefore, the combination of Andersson and Thomas does not teach each and every limitation of claim 1. Accordingly, claim 1 is patentable.

Andersson does not teach or suggest a memory within the body of the portable device that contains “initial identification indicia to initially identify the portable device to the host computing device as a storage device, which is known to the host computing device,” as recited

¹ Dependent claim 29 includes a processing unit limitation similar to amended claim 1, and thus is patentable for at least the same reasons as claim 1.

in claim 1. The Patent Office admits that Andersson does not teach “initial identification indicia to initially identify the portable device to the host computing device as a **storage device**, which is known to the host computing device,” but asserts that paragraph 0020 of Andersson teaches a mobile device having a smart card, which is known to have storage (Office Action mailed August 2, 2007, p. 4). Applicant respectfully disagrees.

First of all, paragraph 0020 of Andersson does disclose a smart card. However, the smart card disclosed in Andersson is an external smart card. There is no indication in Andersson that the smart card is in the mobile phone. Thus, the smart card of Andersson cannot contain the claimed initial identification indicia, which is in a memory within the body of the portable device of the claimed invention. Second, there is no suggestion in Andersson that the smart card contains storage. The Patent Office alleges that smart cards are known to have storage, but provides no evidence to support this allegation. Finally, even if smart cards are known to have storage, a point Applicant does not concede, the external smart card disclosed in Andersson does not teach or suggest the invention as claimed. Claim 1 recites that a memory within the body of the portable device contains “initial identification indicia to initially identify the portable device to the host computing device as a storage device, which is known to the host computing device.” The external smart card of Andersson does not contain anything that initially identifies the mobile phone to a host computing device as a storage device. There is simply no mention that the mobile phone of Andersson is identified as a storage device to a host computing device. Thus, Andersson does not teach or suggest a memory within the body of the portable device that contains “initial identification indicia to initially identify the portable device to the host computing device as a storage device, which is known to the host computing device,” as claimed in the present invention.

The Patent Office also asserts that Thomas at col. 5, lines 25-44 teaches the claimed “initial identification indicia to initially identify the portable device to the host computing device as a **storage device**, which is known to the host computing device,” (Office Action mailed August 2, 2007, p. 4). Applicant respectfully disagrees.

Thomas does disclose a media drive, such as a ZIP drive. Although Thomas may disclose a ZIP drive, it does not teach or suggest a portable device that is initially identified to the host device as a storage device and then configured to act as a cryptographic service provider that provides cryptography services to the host. In contrast to the present invention, Thomas

does not disclose that the ZIP drive is initially identified to the host device as a storage device, and then the same ZIP drive subsequently be configured to act as a cryptographic service provider that provides cryptography services to the host. Andersson likewise does not teach such a portable device. Thus, since neither Andersson nor Thomas teach or suggest a portable device that is initially identified as a known storage device to the host, and then runs configuration software from the portable device on the host device in order that the portable device can serve as a cryptographic service provider, the combination of Andersson and Thomas does not teach each and every limitation of claim 1. Accordingly, claim 1 is patentable.

The combination of Andersson and Thomas also fails to teach or suggest “configuration indicia to subsequently identify the portable device to the host computing device as a cryptographic service provider and provide configuration instructions to allow the host computing device to effectively interact with the portable device as the cryptographic service provider,” as recited in claim 1. The Patent Office alleges that Andersson teaches this limitation in paragraph 0023 (Office Action mailed August 2, 2007, p. 3). Applicant respectfully disagrees.

Paragraph 0023 of Andersson discloses that the mobile phone can be used as an authentication token such that authentication can take place at a Wireless Application Protocol (WAP) Gateway, a modem, and/or a web server. There is nothing in paragraph 0023 of Andersson that teaches or suggests the claimed configuration indicia. Although the mobile phone may be used as an authentication token in Andersson, Andersson does not disclose anything that indicates that the mobile phone is identified to a host computing device as a cryptographic service provider. Andersson also fails to teach or suggest anything that is equivalent to the claimed configuration instructions that allow the host computing device to effectively interact with the portable device as the cryptographic service provider. The Patent Office has failed to point out what it considers to be the claimed host device and has not shown where a host interacts with the mobile phone of Andersson as a cryptographic service provider. In addition, the mobile phone of Andersson is not initially identified to the host as a storage device and then subsequently identified to the host as a cryptographic service provider through the claimed configuration indicia. Thus, Andersson does not teach or suggest “configuration indicia to subsequently identify the portable device to the host computing device as a cryptographic service provider and provide configuration instructions to allow the host

computing device to effectively interact with the portable device as the cryptographic service provider,” as recited in claim 1. Accordingly, claim 1 is patentable for this additional reason.

In addition, neither Andersson nor Thomas teaches or suggests where the portable device includes a processing unit associated with said memory, wherein the service indicia includes instructions for said processing unit to provide the service corresponding to the cryptographic service provider for the host computing device. That is, neither Andersson nor Thomas teaches or suggests a portable device that operates as a hardware-based cryptographic service provider to provide a cryptographic service to the host device. The Patent Office asserts that Andersson, at paragraphs 0040-0042, teaches a processing unit associated with the memory and wherein the service indicia includes instructions for the processing unit to provide the cryptography services for the host computing device (Office Action mailed August 2, 2007, p. 3). Applicant respectfully disagrees.

Andersson discloses using the mobile phone as an authentication token when a user wants to communicate with a remote server (Andersson, Abstract). The mobile phone in Andersson merely acts as an authentication token; it does not operate as a hardware-based cryptographic service provider to provide a cryptographic service to the host device. In fact, the mobile phone in Andersson does not provide a cryptographic service to a host device to which it has initially identified itself as a storage device. In Andersson, the user of the mobile phone authenticates himself to the mobile phone where the mobile phone is acting as an authentication token, and then the token authenticates itself to the authentication server (see Andersson, paragraph 0027, 0028, and 0040-0042). The mobile phone is not providing authentication services to a host device to which it has initially identified itself as a storage device. Therefore, Andersson does not teach or suggest “a processing unit associated with the memory, wherein the service indicia includes instructions for the processing unit to provide the service corresponding to the cryptographic service provider to the host computing device,” as recited in claim 1. Accordingly, claim 1 is patentable for this additional reason.

Claim 17 contains limitations similar to those in claim 1, and is patentable for at least the same reasons set forth above with respect to claim 1. However, claim 17 is slightly different from claim 1. Claim 17 includes the limitations “identifying a portable device to a host computing device as a storage device, which is known to the host computing device”; “registering the portable device with the host computing device as the storage device”;

“automatically identifying the portable device to the host computing device as a cryptographic service provider”; and “enabling the portable device as the cryptographic service provider with the host computing device based on information provided on the portable device.”

As discussed above, the combination of Andersson and Thomas fails to teach or suggest where a portable device is identified to the host computing device as a storage device and then is subsequently identified as a cryptographic service provider. In addition, neither Andersson nor Thomas, either alone or in combination, teaches or suggests where the identifying the portable device as a cryptographic service provider is automatic. The Patent Office cites to paragraph 0023 of Andersson as allegedly teaching “automatically identifying the portable device to the host computing device as a cryptographic service provider” (Office Action mailed August 2, 2007, p. 6). Applicant has reviewed the cited portions of Andersson and finds no teaching or suggestion that the mobile phone of Andersson is automatically identified as a cryptographic service provider.

In addition, although Andersson does disclose that the mobile phone can be used as an authentication token, there is no mention of identifying the mobile phone of Andersson as two different device types (first a storage device and then a cryptographic service provider), as recited in claim 17.

Moreover, Andersson does not teach or suggest that the mobile phone is registered with the host device as a storage device. The Patent Office admits that Andersson does not teach this limitation, but alleges that Figure 4 of Thomas shows this limitation (Office Action mailed August 2, 2007, p. 6). Figure 4 of Thomas indicates that there is a registry associated with a task disk control file (TDCF). The TDCF configures registry information such that the operating system is aware of the path, environmental variables, and commands to launch the participating application (Thomas, col. 8, lines 1-6). The registry in Thomas does not include an indication that a portable device is registered with the host computing device as a storage device, as recited in claim 17. Therefore, Thomas does not teach or suggest “registering the portable device with the host computing device as the storage device,” as recited in claim 17. Thus, for at least these reasons, claim 17 is patentable.

Claims 3, 5, 6, 9-11, and 24-28 depend from claim 1 and contain all the limitations of claim 1. Therefore, claims 3, 5, 6, 9-11, and 24-28 are patentable for at least the same reasons as set forth above with respect to claim 1. Claims 20 and 29-31 depend from claim 17 and contain

all the limitations of claim 17. Therefore, claims 20 and 29-31 are patentable for at least the same reasons as set forth above with respect to claim 17.

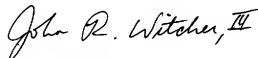
In addition, claims 5 and 30 are patentable for an additional reason. In particular, claim 5 recites that the configuration indicia includes a file executable on the host computing device to reconfigure the host computing device to recognize and interact with the portable device as the cryptographic service provider. Dependent claim 30 has a similar limitation. Neither Andersson nor Thomas, either alone or in combination, teaches or suggests such a limitation. The Patent Office refers to Thomas, Figure 4, as allegedly teaching this limitation (Office Action mailed August 2, 2007, p. 5). Applicant respectfully traverses. Figure 4 of Thomas is a TDCF. This file does contain configuration instructions. However, the TDCF of Thomas does not execute on the host computing device to reconfigure the host computing device to recognize and interact with the portable device as the cryptographic service provider. Accordingly, neither Thomas nor Andersson, either alone or in combination, teaches or suggests a portable device "wherein the configuration indicia includes a file executable on the host computing device to reconfigure the host computing device to recognize and interact with the portable device as the cryptographic service provider," as recited in claim 5. Therefore, claim 5 and claim 30, which contains a similar limitation, are separately patentable for this additional reason.

The present application is now in condition for allowance and such action is respectfully requested. The Examiner is encouraged to contact Applicant's representative regarding any remaining issues in an effort to expedite allowance and issuance of the present application.

Respectfully submitted,

WITHROW & TERRANOVA, P.L.L.C.

By:



John R. Witcher, III
Registration No. 39,877
100 Regency Forest Drive, Suite 160
Cary, NC 27518
Telephone: (919) 238-2300

Date: November 1, 2007
Attorney Docket: 4989-009